The Sun™ Infrastructure Solution for Secure Network Access Platform

High Assurance Thin Client Access to Multiple Security Domains

Technical White Paper

Sun Microsystems, Inc.

THIS PUBLICATION IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

Table of Contents

Preface

Purpose

In certain government organizations, security policy dictates that classified information must be restricted and isolated within precise security boundaries. Users must have the appropriate clearances to access sensitive information and the computers, networks, and applications within the perimeter of each secured area.

The Secure Network Access Platform for Government provides a single desktop that securely controls access to compartmentalized IT resources. For many government customers who run applications at different security levels or compartments, implementing the Secure Network Access Platform Reference Architecture can greatly simplify user access, reduce IT acquisition and maintenance costs, enhance availability, and improve inter-agency collaboration.

The Secure Network Access Platform for Government was created under a Sun initiative known as Sun Infrastructure Solutions, which strive to simplify the delivery of complex, enterprise-wide, networked computing systems. This solution encompasses a set of software and hardware components that Sun has integrated into a proof-of-concept environment. Customers can leverage this solution to reduce implementation complexity, minimize risk, and shorten time-to-deployment. The Secure Network Access Platform is designed to help organizations decrease complexity and risk, and can contribute to a lower overall total cost of ownership (TCO).

Scope

This guide gives a technical overview of the Secure Network Access Platform solution, describing its hardware and software components. It explains the architectural model, highlights solution benefits, and discusses design considerations.

Audience

The Secure Network Access Platform Reference Architecture is targeted at government customers and integrators that must access multiple security compartments (such as defense, intelligence, and homeland security agencies). This paper is intended for an audience of technical decision-makers, IT professionals, and consultants in these environments. A secondary audience is Sun sales representatives, systems engineers, and Sun Services consultants who support government customers, contractors, and integrators.

Introduction

Challenges in Implementing Compartmentalized Security

In classified government operations, security requirements often dictate the need for strict separation and isolation of sensitive information. Typically, different government programs are segregated into restricted security compartments. Individuals must hold the appropriate clearances to have access to facilities, computing resources, networks, applications, and data that are classified into each specific level and compartment. The intent is to protect information – to insulate it from unauthorized penetration, and to prevent inadvertent error that might compromise agents or operations.

In these environments, it is a common security practice to enforce a tightly controlled “air gap” – a physical separation – between computing resources and networks that host classified applications in each compartment. As a result, a “stovepiped” application architecture often results in which multiple dedicated PC desktops and networks provide separate access points to multiple security compartments (Figure 1).

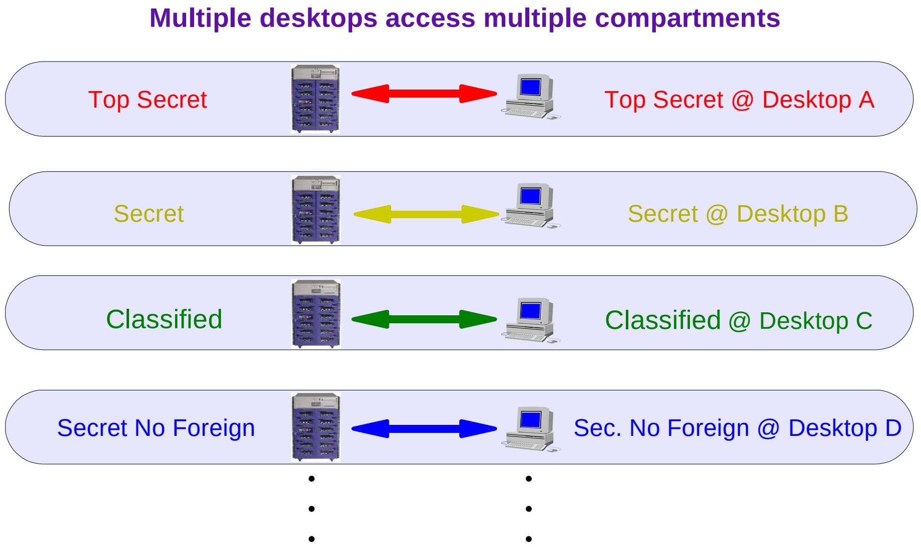


Figure 1. Security requirements often result in a “stovepiped” application architecture.

A “stovepiped” architecture tends to inhibit collaboration between multiple government agencies at a time when enhanced collaboration is increasingly desirable. In the U.S. defense and intelligence communities, there is a heightened need to share information related to certain classified operations with international coalition partners. To access multiple compartments in a "stovepiped" application architecture, users are forced to access several different physical PC desktops, sometimes in different physical locations. Not only is this an inconvenience, but it can inhibit users from easily synthesizing information obtained from multiple sources. Multiple access points may not only decrease agent productivity, but they may lessen effectiveness as well.

"Fat" Client Issues

In many classified environments, additional challenges are posed by the use of "fat" client PC platforms. Most notably, Microsoft Windows/NT-based operating systems are the frequent targets of computer viruses and worms, which can impact mission-critical system availability and degrade user productivity. Recently, a worm virus attacked the U.S. State Department's Consular Lookout and Support System (CLASS), a tool used in the visa approval process to help prevent terrorists from gaining entrance to the United States. Efforts to contain the worm attack resulted in a systems outage that severely impacted operations.[1]

In some highly classified environments, the repair of PC platforms can also be problematic – in some cases disks must be "sanitized" (wiped clean of all data) or even destroyed before they can be removed from the premises. When repairs are complete, PC disks must then be rebuilt with an operating system and applications, adding to an already heavy administrative workload. Since PC systems are "stateful" (that is, they are individually loaded with user applications and data), they require a huge investment in systems administration. Stateful desktops also inhibit user mobility. A user that switches to a different desktop PC system cannot automatically access the same compute environment and applications.

In the stovepiped model, desktops and networks are replicated at each security level to ensure isolation, escalating infrastructure acquisition and maintenance costs. Since PC desktops require high levels of administrative support, these fat-client environments typically suffer from high maintenance costs and a high total cost of ownership (TCO).

[1] For more details, see "Virus Strikes State Department", CNET News, September 24, 2003, currently available at http://zdnet.com/2100-1105_2-5081360.html.

The Secure Network Access Platform Reference Architecture and Single Desktop Access

The Secure Network Access Platform (Secure Network Access Platform) Reference Architecture defines a single desktop that provides controlled access to multiple security compartments. This architectural model eliminates the duplication of IT resources, simplifies user access, reduces IT administration, enhances availability, and improves a user's ability to integrate data from multiple sources – all while strictly enforcing security policy. The Secure Network Access Platform leverages the heterogeneous IT infrastructure, allowing users to run familiar Windows 2000/NT applications such as Microsoft Office along with legacy X Windows-based applications.

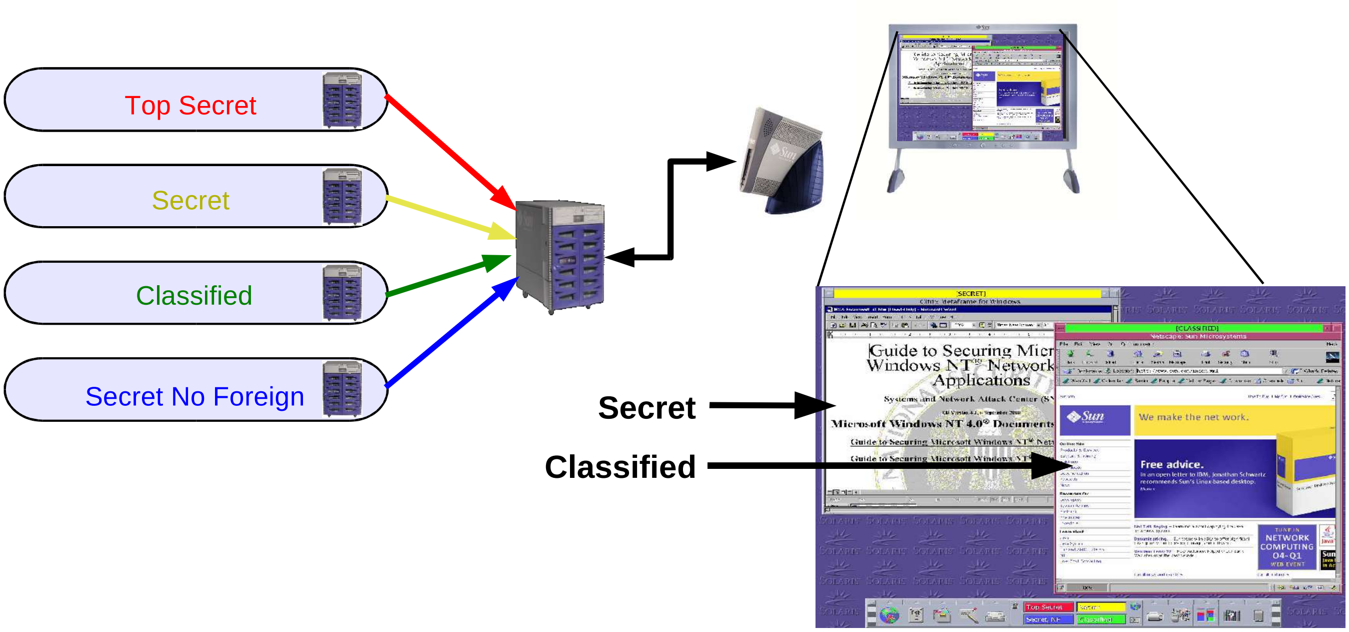


Figure 2. Secure Network Access Platform provides a single desktop with secure access to multiple compartments.

As shown in Figure 2, the Secure Network Access Platform allows a user to access different compartmentalized applications from a single desktop – from a diskless, stateless “ultra-thin” networked appliance. The Secure Network Access Platform provides the necessary security containment, isolating sensitive data and system resources and granting users access to each application and network only if they hold the appropriate clearances. The architecture supports users who must access different compartments within a single classified level, or those who must access multiple security classifications and compartments.

Security policy is enforced through Mandatory Access Control (MAC) labels, which cannot be changed by unauthorized users. (This is in contrast to Discretionary Access Control (DAC) restrictions provided in standard operating systems, where the data's owner can modify access control settings.) In the Secure Network Access Platform , MAC labels are created by the Trusted Solaris™ Operating Environment, a key software component. The Trusted Solaris Operating Environment applies labels pervasively and automatically to all data objects and information flows, including networks, packets, files, directories, windows, memory, processes, and interprocess communication mechanisms.

Label names and relationships are defined in a Trusted Solaris Operating Environment database. Label names consist of two components:

- A hierarchical classification called a sensitivity label (e.g., “Top Secret,” “Secret,” “Confidential,” “Unclassified”)
- Zero or more compartments known as information labels, which are often program names or other logical identifiers

To access multiple security compartments from a thin-client appliance, the user initiates each browser-based application at a MAC label appropriate for accessing the secure network. If the user holds a clearance that dominates the MAC label, then he or she is granted access to the network and application at that label. Otherwise, access is denied and the unsuccessful attempt is typically recorded in the audit trail.

If access is granted, the application is displayed in a window clearly labeled with a security banner that shows the MAC label. Figure 3 shows an example of several labeled windows as they might appear on a Sun Ray™ thin client. Note that label banners are displayed in different colors to help users easily distinguish between applications at different levels or in different security compartments.

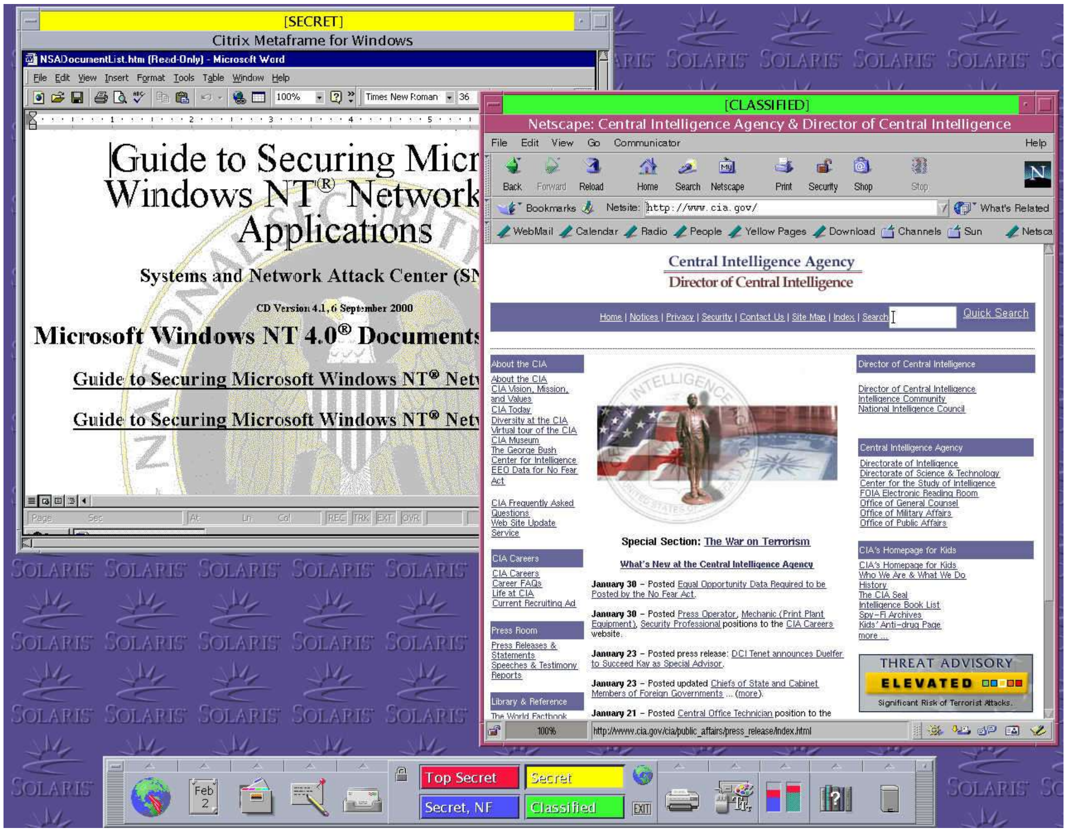

[SECRET]
Citrix Metaframe for Windows
NSADocumentList.htm (Read-Only) - Microsoft Word
Guide to Securing Microsoft Windows NT Network Applications
Systems and Network Attack Center (SNAC)
CD Version 4.1, 6 September 2000
Microsoft Windows NT 4.0® Documents
Guide to Securing Microsoft Windows NT® Network
Guide to Securing Microsoft Windows NT® Network
[CLASSIFIED]
Netscape: Central Intelligence Agency & Director of Central Intelligence
Netsite: http://www.cia.gov/
Central Intelligence Agency
Director of Central Intelligence
Special Section: The War on Terrorism
THREAT ADVISORY
ELEVATED
Significant Risk of Terrorist Attacks
Top Secret
Secret
Secret, NF
Classified
SOLARIS

Figure 3. Windows on Secure Network Access Platform thin clients can be clearly labeled with security banners.

Key Capabilities

The Secure Network Access Platform features these key capabilities:

- Security containment. Containment is a critical requirement when hosting applications with multiple compartments on the same desktop and within the same infrastructure – it must not be possible for applications to interfere with each other or to access another application's data. The Trusted Solaris Operating Environment implements mechanisms that provide the necessary containment, with high assurance and strength of protection.
- Single access point. Trusted windowing enables the consolidation of compartments on the same desktop and prohibits application communication. Downgrading information via "cut and paste" operations between windows is prohibited unless the user is specifically authorized to perform this privileged operation.

- Network separation. In the Secure Network Access Platform Reference Architecture, a single thin client desktop can access compartmentalized networks without security compromise. Trusted Solaris routes an outgoing packet only through an interface with an accreditation range containing the packet's label – otherwise the packet is dropped. An incoming packet is dropped unless it is within the accreditation range of the interface on which it is received. In the Secure Network Access Platform, Trusted Solaris is configured to assign MAC labels to packets on trusted and untrusted networks according to each network interface. Firewall capabilities in SunScreen™ software block unauthorized network packets and enhance network isolation.

- No desktop administration. The Secure Network Access Platform eliminates desktop administration since Sun Ray thin clients are completely stateless – they have no locally resident data, applications, or operating system that must be upgraded or annually re-licensed. Virtually no administration is required to add, move, or exchange them, and users can access the same compute environment from any Sun Ray thin client on the LAN.

- Compatible with existing applications and networks. The Secure Network Access Platform is designed to coexist within an existing heterogeneous infrastructure. Familiar Microsoft Windows and X Windows applications on different classified networks are available to the user, conveniently co-located on a single desktop.

- Auditing. Auditing can be configured to track all or selected user events. The security analyst uses an intuitive graphical user interface to define how auditing should occur on each server running the Trusted Solaris Operating Environment.

Business Benefits

Lower Total Cost of Ownership

Lowering the total cost of ownership (TCO) is an increasingly high priority for IT management. In classified security environments, sky-rocketing costs of administration and maintenance are often compounded by the duplication of desktop and network resources. The Secure Network Access Platform eliminates desktop maintenance and centralizes other administrative tasks through the use of thin client computing. Since Sun Ray clients are "ultra-thin"– they have no local disk, applications, or operating system – a single administrator can easily manage well over 1,000 clients.

Sun Ray thin clients are simple, always-on, low-cost devices that require no annual desktop refresh costs but yet can provide a familiar user experience. Unlike Microsoft Windows-based PCs, they do not need to be upgraded when new applications are introduced or more computing power is required. They enhance mobility, allowing users to move to any client on the same LAN and access the same applications. Sun Ray thin clients also have no moving parts, virtually eliminating desktop repairs – if a desktop unit fails, it can be simply swapped for another. Most importantly, Sun Ray thin clients are not prone to virus and worm attacks that can cripple PC-based installations, decrease user productivity, and disable operations.

Improved Collaboration

Stringent security measures can sometimes seem counterproductive in intelligence and defense operations where information sharing can be a benefit. The Secure Network Access Platform promotes crosstalk between government agencies and coalition partners while maintaining and enforcing security policy. Since cleared users can conveniently access multiple security compartments on the same desktop, the architecture can help to improve inter-agency collaboration and data synthesis.

A user with appropriate clearances, for example, can access intelligence applications from one network, defense data from another, Homeland Security information from a third, and unclassified data from the Internet. Coalition partners with appropriate clearances can access applications and data from various compartments. Applications from each network are clearly labeled so the user can readily identify security classifications and compartments while working. The Secure Network Access Platform safely contains data within each application window and network, enforcing security isolation and preventing unauthorized data access.

Reduced Risk

A systems vendor experienced in developing network computing solutions, Sun created the Secure Network Access Platform as a part of the Sun Infrastructure Solutions initiative. Sun Infrastructure Solutions encompass the essential solution elements that are needed to deliver applications throughout an infrastructure – from the workgroup through the data center. Designed to reduce deployment risk, Sun Infrastructure Solutions represent proven and tested solutions – ones that have been previously architected, implemented, and managed using Sun iForce Centers and customer environments. Each solution includes a reference architecture, best-practice methodologies, documentation, and Sun service offerings.

To build a reference implementation for the Secure Network Access Platform Reference Architecture, Sun engineers combined industry-leading technology components from Sun and iForce partners in a proof-of-concept setting. The Secure Network Access Platform Reference Architecture provides a proven design methodology that combines flexibility with predictable results, allowing customers to deploy more quickly and with less risk. Sun Services consultants can provide the necessary network computing and implementation expertise to apply and augment the solution.

The Secure Network Access Platform Reference Architecture is based on best practices from key Sun customers, such as the Joint Intelligence Center of the Pacific (JICPAC) in Honolulu, HI which provided the business and technical requirements necessary to create the solution. JICPAC has consolidated multiple PC clients onto single Sun Ray clients, while meeting both their security and cost savings goals.

High Assurance – Independent Certification

Independent software evaluations are conducted to verify vendors' security claims and to ascertain any security vulnerabilities that may exist. The governments of the United States and the United Kingdom – along with Australia, Canada, France, Germany, and New Zealand – have mutually agreed to recognize evaluations from the Common Criteria organization.

The Trusted Solaris Operating Environment is the only commercially available operating environment that is independently certified under the Common Criteria scheme at the EAL4 level with the following profiles: Role Based Access Protection Profile (RBACPP), Labeled Security Protection Profile (LSPP), and Controlled Access Protection Profile (CAPP). The EAL4 level of evaluation with this collection of protection profiles is unmatched by any other operating system on the market. The Trusted Solaris Operating Environment provides strict security containment and enforcement in the Secure Network Access Platform Reference Architecture.

Overview of the Secure Network Access Platform

The Secure Network Access Platform is based on an N-tiered software architecture. Figure 4 shows an overview of the services provided at various layers in the solution stack, and introduces some of the solution components.

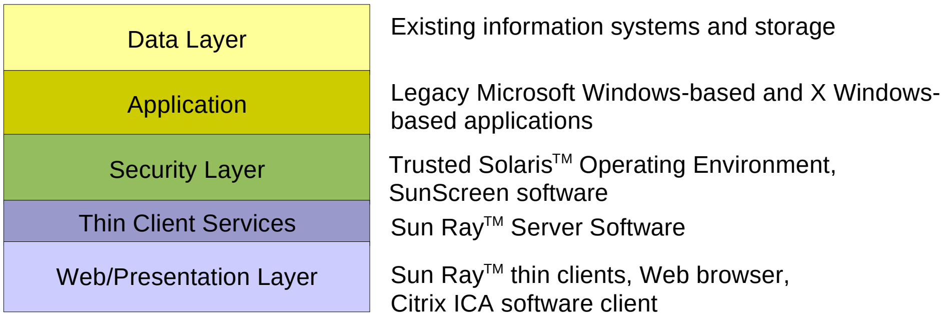

Data Layer
Existing information systems and storage
Application
Legacy Microsoft Windows-based and X Windows-based applications
Security Layer
Trusted SolarisTM Operating Environment, SunScreen software
Thin Client Services
Sun RayTM Server Software
Web/Presentation Layer
Sun RayTM thin clients, Web browser, Citrix ICA software client

Figure 4. Service layers in the Secure Network Access Platform Reference Architecture.

At the top of the stack is the existing data storage in each classified network. The Secure Network Access Platform does not impact the Data Layer but provides secure compartmentalized access to these existing data resources.

At the Application Layer, the Secure Network Access Platform provides access to legacy Microsoft Windows applications and X Windows-based applications. Often the Citrix MetaFrame server software already exists in the infrastructure. With the Citrix client software in the Presentation tier, the Citrix MetaFrame server allows users to run Windows-based applications such as Microsoft Office from a Windows Server. Legacy X Windows-based applications can also be remotely displayed on the thin client desktops.

One notable difference between the Secure Network Access Platform and many other networked computing architectures is a security services tier interjected between the Presentation and Application Layers. The Security Layer permits polyinstantiation of system resources at various security levels and compartments, and restricts access to those resources according to user clearances and process privileges. The Security Layer also tracks security-related events, recording them in the audit trail. The Trusted Solaris Operating Environment is the primary component at this layer, with SunScreen software providing additional network filtering.

In conjunction with the Presentation tier is a sub-layer supporting thin client services. The Sun Ray™ Server Software performs all computing for the Sun Ray thin clients, generating pixel data that is transmitted to the thin client displays. At the bottom of the stack, the Web/Presentation Layer contains the Sun Ray "ultra-thin" clients themselves, the Web browser, and the Citrix client software.

Physical Infrastructure

Figure 5 shows how the layers of the software stack are mapped onto a physical infrastructure. On the Sun Ray thin clients, users with the appropriate clearances can execute applications simultaneously on four different compartmentalized networks – labeled Top Secret, Secret, Classified, and Secret No Foreign.

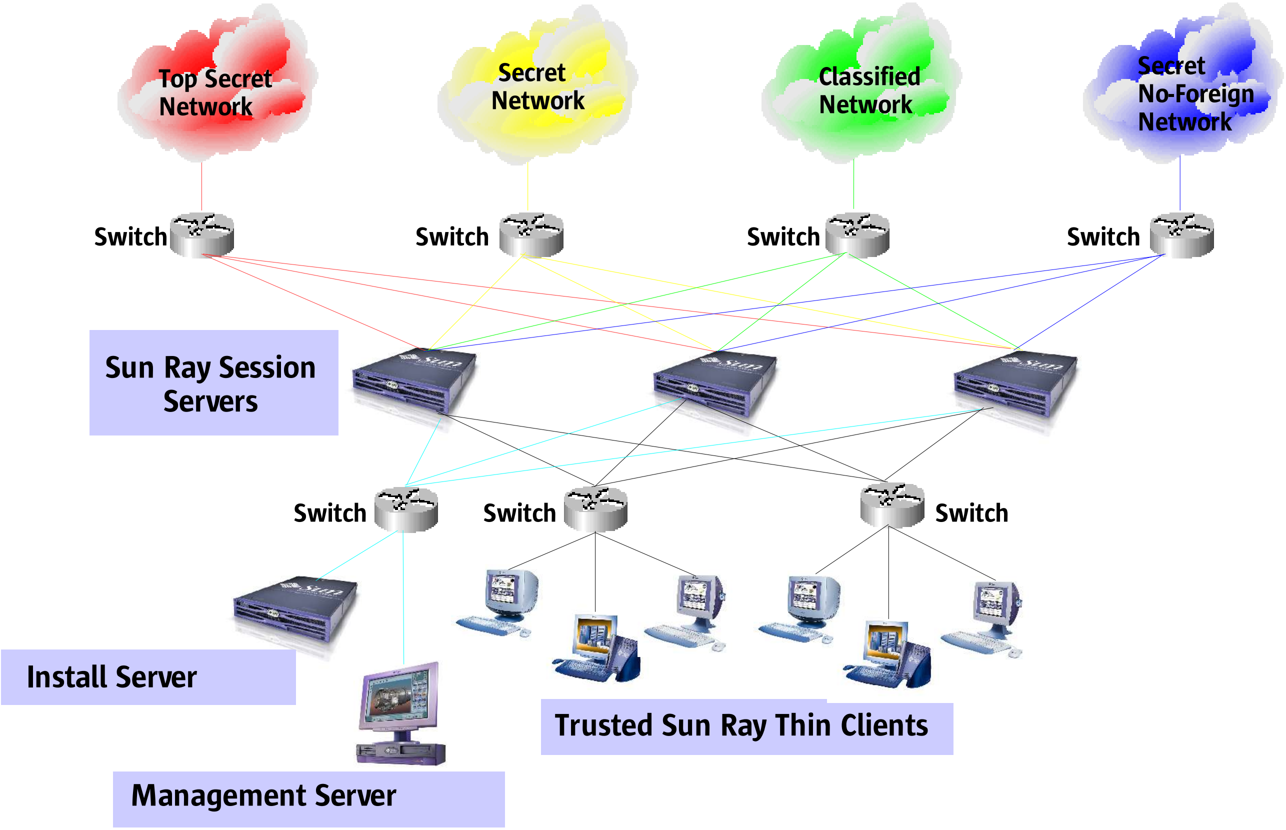


Figure 5. Architectural layout and Secure Network Access Platform components.

Server Infrastructure

In Figure 5, powerful, reliable, and affordable Sun Fire V240 servers host the principal software components. Sun Fire V240 servers are used in the Secure Network Access Platform in two key roles:

- as Secure Network Access Platform Sun Ray Session Servers, hosting the Trusted Solaris Operating Environment, Sun Ray server software, SunScreen software, and Citrix ICA client software
- as Secure Network Access Platform Install Servers, hosting the Trusted Solaris Operating Environment and leveraging Solaris JumpStart technology to facilitate installation

Sun Ray Session Servers host the Citrix ICA client software that allows Sun Ray thin clients to run Windows 2000/NT applications. The Secure Network Access Platform architecture also supports X Windows-based applications, including Solaris X Windows-based applications using Trusted Solaris X Windows extensions. Applications access existing storage resources in each isolated classified network. The Sun Ray Session Servers are responsible for labeling windows displayed on the thin clients.

Networking Infrastructure

Each Sun Ray Session Server connects to each and every classified network, as shown in Figure 5. If a Sun Ray Session Server receives unlabeled packets from a trusted network, it can impose an appropriate MAC label on packets from that network interface. SunScreen software provides additional packet filtering, blocking unauthorized network access and enhancing network isolation.

Gigabit Ethernet switches are used to simplify cabling and configuration. Two tiers of switches provide the necessary network connections. One tier connects Sun Ray Session Servers to the classified networks, while another connects Sun Ray thin clients to each Sun Ray Session Server in a Sun Ray failover group. Switched 100Base-T links are recommended between the Sun Ray thin clients and the Gigabit switch.

The switches that attach to the back-end classified networks route packets from the Sun Ray Session Servers to the appropriate classified networks. The Trusted Solaris Operating Environment and SunScreen software provide the necessary network containment and isolation consistent with security policy.

Provisioning

Part of the inherent value of the Secure Network Access Platform is the provisioning methodology developed to deploy it. Built-in Solaris JumpStart capabilities are used to simplify Sun Ray Session Server installations. JumpStart technology can help administrators replicate server configurations more quickly and more precisely, especially in large implementations. The next section describes this provisioning methodology and the hardware and software components in more detail.

Secure Network Access Platform Components

The Secure Network Access Platform integrates the following hardware and software components:

- Trusted Solaris™ 8 HW 7/03 Operating Environment, Certified Edition
- SunScreen™ 3.2 software (included with Trusted Solaris 8 HW 7/03 Operating Environment release)
- Sun Ray™ Enterprise System components, including:
  - Sun Ray Thin Clients
  - Sun Ray Server Software 2.0
  - Network interconnects for Sun Ray Thin Clients
- Sun Fire V240 Servers
- Sun Blade 150 Workstation
- Citrix MetaFrame XP Presentation Server for Windows (Feature Release 3) and ICA Client 7.02 for Solaris
- Solaris JumpStart for provisioning

The remainder of this section describes each component and its role in the reference architecture. Sun selected these components to meet design criteria for security, high availability, performance, scalability, and manageability. The next section describes how the components meet these design goals.

Trusted Solaris Operating Environment

The Trusted Solaris Operating Environment follows the Bell-LaPadula security model that was first developed in 1973 for the U.S. Air Force to address multi-level security requirements. The Bell-LaPadula model stipulates that access by a subject (a user or process) to an object (a file, a network packet, or any other piece of data) should be allowed or disallowed based on a comparison of the object's security classification and the subject's security clearance. The Trusted Solaris Operating Environment implements this model by imposing Mandatory Access Control labels on system and data objects, along with user clearances and authorizations.

The Trusted Solaris 8 Operating Environment is based on the scalable Solaris 8 Operating Environment, and includes the following features:

- Reduced Risk of Security Violations

The combination of object labeling, clearance levels for each user, and strong auditing capabilities holds all users accountable and all actions traceable, greatly diminishing the risk of security violations. The Trusted Solaris 8 Operating Environment uses the security principle of least privilege, which restricts users to only those functions necessary to perform their jobs.

- Increased Assurance

Mandatory Access Controls allow information to be processed in multiple security compartments, and enables file sharing for users in the same compartment. Administrators can label printer output, restrict access to individual printers, and limit who can view print queue information.

- More Granular User Control

Role-Based Access Control (RBAC) divides administrative tasks among a number of roles and grants only the necessary authority to perform the related tasks. RBAC ensures that all administrative actions are traceable to an authenticated individual instead of to just a single root user, which provides greater accountability. By convention, Trusted Solaris defines a System Administrator role to perform administrative tasks, and a Security Administrator role to perform security-related tasks. Trusted Solaris also maintains a hierarchical database of Rights Profiles that define the set of applications and privileges needed for each user.

- Protection of Local Devices

Administrators can prohibit access to local devices, such as locking down USB ports on thin clients. Pluggable Authentication Modules can provide failed-login account locking, trusted-path checking, and machine-generated passwords without the need to change source code.

- Independent Certification – Common Criteria

Sun products have successfully passed many government-sponsored and independent evaluation programs. The Trusted Solaris Operating Environment has passed Common Criteria certification at EAL4 with the RBACPP, LSPP, and CAPP protection profiles – an evaluation level unparalleled by any other commercially available operating system.

The Trusted Solaris Operating Environment provides a hardened platform for customers that must strictly control access to sensitive information. In the Secure Network Access Platform architecture, Trusted Solaris acts as a highly secure and auditable gateway between trusted and untrusted domains in large, heterogeneous classified networks.

SunScreen Software

In the Secure Network Access Platform, the SunScreen software is installed on Sun Ray Session Servers to isolate networks and enhance network security. The SunScreen software acts as a firewall and screens packets according to a set of pre-established rules. At installation, the System and Security Administrators define these rules in accordance with site security policy.

Sun Ray Enterprise System

The components in a Sun Ray Enterprise System include:

- Sun Ray Ultra-Thin Clients
- Sun Ray Server Software 2.0, which provides user authentication, user session management, static load distribution, and failover group management for thin clients
- A high-speed interconnect between one or more Sun Ray servers and the Sun Ray thin clients
- One or more Sun Fire servers running the Trusted Solaris 8 HW 7/03 Operating Environment, Certified Edition

Sun Ray Ultra-Thin Clients

Sun Ray Ultra-Thin Clients – which consist of a client, a monitor, a keyboard, a mouse, and a built-in smart card reader – can provide seamless access to workstation and PC applications. Since there is no local memory or local computing power on Sun Ray thin clients, the actual computing is performed on the remote Sun Ray Session Servers (Figure 5).

Features of a Sun Ray thin client include:

- 24-bit, 2D accelerated graphics up to 1280x1024 resolution at 85 Hz (640 x 480 at 60 Hz is the lowest supported resolution)
- Multichannel audio input and output capabilities
- Smart card reader (use is optional in the Secure Network Access Platform Reference Architecture)
- USB ports that support hot-pluggable peripherals
- EnergyStar compliance
- No fan, switch, or disk
- Very low power consumption

The Sun Ray thin client acts as a frame buffer on the client side of the network. Applications render their output to a region of memory on the Sun Ray Session Server that contains the current state of each user's display. The Sun Ray Server Software formats and sends the rendered output to the appropriate thin client, where the output is interpreted and displayed.

From the point-of-view of the network, Sun Ray appliances are identical except for their Ethernet addresses, which greatly simplifies repair and replacement. When the thin client is connected to the network and booted, it is assigned an IP address via DHCP, and a thin client session is created on the Sun Ray Session Server.

Sun Ray Server Software

The Sun Ray Server Software 2.0 hosts user sessions for the Sun Ray thin clients. The software provides four key capabilities:

- Session failover. The Sun Ray Server Software provides support for multiple servers to manage a set of connected Sun Ray thin clients. Defining a set of servers as a "failover group" provides for automatic user re-authentication on another Sun Ray Session Server if one server in the failover group becomes unavailable. (Note that failover occurs at the user authentication level and that user applications hosted on the server do not fail over.)
- Hot desking. "Hot desking" refers to a user's ability to access applications from any thin client on the LAN. Because Sun Ray thin clients are stateless, a user's session can be redirected to any Sun Ray thin client on the LAN when the user inserts his or her token card – the session "follows" the user to the new thin client. (Hot desking requires the use of a smart card in Secure Network Access Platform implementations.)
- Load balancing. The Sun Ray Server Software provides static load distribution. When a new thin client session is initiated, the session can be placed on any one of the servers in the group based on the availability of server resources. The load balancing algorithm takes into account each server's load and capacity (the number and speed of its CPUs) so that larger or less heavily loaded servers can host more sessions.
- Encryption. Sun Ray Server Software 2.0 supports the ARCFOUR encryption algorithm, enabling the encryption of traffic between Sun Ray Session Servers and Sun Ray desktop units.

Session mobility and failover capabilities translate to an "always on, always available" desktop resource for users anywhere in their workgroup or on the corporate LAN. This frees the user from an individual desk or machine, which is increasingly important as office sharing becomes more prevalent.

The Sun Ray Server Software has these five components:

- Authentication Manager, which recognizes and validates Sun Ray users in conjunction with Trusted Solaris authentication mechanisms (e.g., via NIS, NIS+, or files).
- Group Manager, which keeps track of failover group membership, facilitates server selection and redirection, and performs static load distribution of thin client sessions.
- Session Manager, which maps a user session on a server to a physical Sun Ray thin client, and binds/unbinds related services to and from the specific client.
- Administration Tool, which supports user management and usage monitoring.
- Firmware Download Mechanism, which determines whether the firmware in a Sun Ray thin client matches that of the Sun Ray Server Software, and provides updates. (Automatic firmware updating can also be disabled.)

When a thin client user is authenticated, a session is directed to a Sun Ray Session Server in the failover group. The Group Manager determines which server should host the user session, based on system resources and the current server load.

Interconnect for Sun Ray Thin Clients

To provide responsiveness, a high-speed interconnect is needed between Sun Ray Session Servers and the Sun Ray thin clients. Within a failover group, every Sun Ray thin client must have a path through the interconnect fabric to every Sun Ray Session Server. A Gigabit Ethernet switch is recommended to connect all the servers in the failover group (refer back to Figure 5). Switched 100Base-T links are recommended between the Sun Ray thin clients and the Gigabit Ethernet switch. This configuration guarantees ample interconnect bandwidth and provides connectivity within the failover group without requiring redundant NICs in the servers.

Sun Fire V240 Servers

Combining features for high availability, ease-of-management, and low total cost of ownership (TCO), Sun Fire V240 servers help to deliver affordable data center functionality for Secure Network Access Platform implementations. Packaged in a compact 2U form factor, these low-cost servers are designed for high-density, rack-centric data center applications. Four built-in Gigabit Ethernet ports and additional PCI expandability make these servers ideal for Secure Network Access Platform deployments requiring multiple network connections.

Sun Fire V240 servers feature up to two 64-bit UltraSPARC IIIi processors at 1GHz, with 1MB of internal Level 2 cache per processor, and can support up to 8GB of RAM. Sun Fire V240 servers are binary compatible with the entire Sun family of SPARC-based platforms, including the 106-processor Sun Fire 15K servers. Binary compatibility means that the same applications can run unchanged across the full range of Sun SPARC- and Solaris-based servers.

The following table summarizes features of the Sun Fire V240 server:

Feature	Sun Fire V240 Server
Maximum Memory	8GB
Maximum I/O Slots (cPCI/PCI)	3 PCI (1 @ 66MHz, 2 @ 33MHz)
Maximum # network interfaces	12 (4 on-board Gigabit Ethernet ports plus 2 Sun Quad Fast Ethernet PCI adapters can be added)
Storage	4x73GB internal UltraSCSI

Feature	Sun Fire V240 Server
Availability Features	Hot-swap disks, redundant power supplies, Advanced Lights Out Management
System Management	Sun Management Center 3.0 software, Solaris Management Console

Sun Fire V240 servers are extremely expandable, supporting a wide range of peripherals and expansion opportunities. Standard expansion ports include:

- Gigabit Ethernet – Four built-in auto-negotiating 10/100/1000BaseT ports provide high-speed, high-bandwidth networking
- Ethernet Management – A separate 10BaseT Ethernet port provides a network interface for out-of-band management
- Serial – A DB9 serial port allows connection to terminal servers or other devices
- Serial Management – An RJ-45 serial port provides a console port as well as an out-of-band serial management interface
- USB – Two USB ports support ZIP drives and other peripherals
- SCSI – An external Ultra 160 SCSI port enables the connection of disk arrays and other high-speed storage devices
- PCI – Three full-length PCI slots are available, for example, to provide additional network expansion

To support applications requiring high service levels, Sun Fire V240 servers include the following RAS features:

- Redundant, hot-swappable power supplies with independent power cords
- Hot-swappable, front-accessible disk drives, with software mirroring
- Easy serviceability with front and rear LEDs, no side access required, and a removable host ID

In addition, the Sun Fire V240 servers offer an enhanced manageability feature called Advanced Lights Out Management (ALOM). ALOM leverages a new system controller that supports remote system monitoring, logging, and alert processing, and enables remote out-of-band management. In the Secure Network Access Platform Reference Architecture, authorized system managers can use ALOM to monitor Sun Fire V240 servers, which can facilitate more proactive management, higher service levels, and lower TCO.

Sun Blade 150 Workstation

In the Secure Network Access Platform reference implementation, a single Sun Blade 150 workstation is used as a NIS+ replica server and, optionally, as a management station. The Sun Blade 150 workstation offers considerably high performance in an affordable workstation package. It is a 64-bit workstation with a single 550 MHz or 650 MHz UltraSPARC IIi CPU, up to 2 GB of RAM, one or two 73-GB disk drives, and 2D/3D graphics options for multi-display support.

The Sun Blade 150 workstation is loaded with the Trusted Solaris Operating Environment and used to host a replica of the NIS+ name service database. In addition, optional Sun Management Center software can be installed to monitor the health and resources of all Secure Network Access Platform Sun Ray Session Servers and Secure Network Access Platform Install Servers on the network.

Citrix ICA Client Software

Citrix Systems, Inc. offers a solution that provides interoperability with Microsoft Windows 2000/NT environments and centralizes management of Windows-based applications. In the Secure Network Access Platform Reference Architecture, the Citrix software allows thin-client users to access Windows-based applications from a Windows Server. The Citrix software supports most custom or commercially packaged Windows-based applications, including the popular Microsoft Office applications.

The Citrix software is based on the Independent Computing Architecture (ICA) protocol, which was originally developed by Citrix Systems, Inc. ICA is similar to RDP (Remote Desktop Protocol), the native connection method that Microsoft provides to access Windows Servers.

The Citrix solution consists of both a client and a server component (Figure 6). The server component, Citrix MetaFrame, is an add-on product for Microsoft Windows Server environments. In the Secure Network Access Platform Reference Architecture, the Citrix ICA client resides on the Secure Network Access Platform Sun Ray Session Servers.

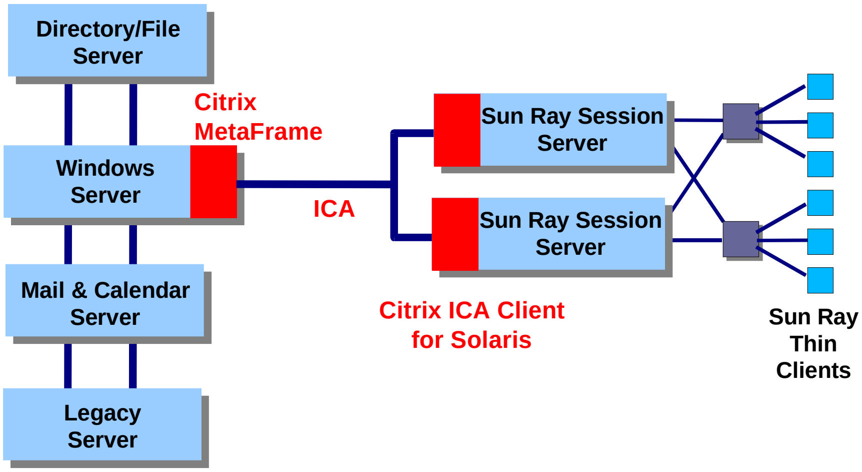


Figure 6. Citrix provides interoperability using a client/server approach.

The Citrix ICA client for Solaris allows native or web-based execution of Windows applications. The ICA client software can integrate with the Sun Ray CDE desktop, allowing a CDE file type to be associated with a specific application published within Citrix MetaFrame.

Solaris JumpStart Technology

Native to the Solaris and Trusted Solaris Operating Environments, JumpStart technology uses an install server to deliver operating system packages to target machines over a local network. JumpStart bases package delivery to installation clients according to customized machine profiles. It can execute pre- and post-installation scripts that can back-up an existing server, add patches, and otherwise fine-tune configurations in a consistent fashion.

Solaris JumpStart technology allows customers to replicate server configurations more easily and more precisely in large implementations. It can automate, for example, the installation of the Trusted Solaris Operating Environment, and duplicate Trusted Solaris database files containing label definitions, network configurations, and user rights profiles. JumpStart can make the installation process more deterministic, shortening the time to takes to deploy, add, or recover servers. To leverage JumpStart technology in large Secure Network Access Platform deployments, Sun recommends that customers and system integrators engage experienced Sun Services consultants.

Integrating Secure Network Access Platform Components

To develop the Secure Network Access Platform, Sun picked best-of-breed solution components that can contribute to high assurance of security, reduced risk, and lower TCO. In particular, Sun looked for components that facilitate availability, ease of management, and simplified administration, while enforcing security containment and isolation.

Sun engineers integrated the selected Secure Network Access Platform components in a functional proof-of-concept demonstration, evolving a server provisioning methodology to help accelerate server installation, speed recovery, and enhance configuration consistency. This provisioning methodology, along with experienced Sun Services consultants, can help reduce risk and slash time-to-deployment for implementations based on the Secure Network Access Platform.

Secure Network Access Platform Design Criteria

This section looks at a number of design criteria addressed by the Secure Network Access Platform, including security, high availability, performance, scalability, and manageability.

Security

The Secure Network Access Platform provides security compartmentalization through the Trusted Solaris Operating Environment. Trusted Solaris has been implemented in many government agencies that have stringent classified security requirements – it has also been implemented in private sector businesses (such as in financial services and healthcare) to support data separation and privacy. The combination of object labeling, user clearance levels, and privileges creates an environment that isolates applications and data, enforcing site security policy. Strong audit capabilities hold users accountable and all actions traceable, greatly lessening the risk of security violations. To further enhance security in implementations of the Secure Network Access Platform, SunScreen software provides additional packet filtering. Optionally, traffic between Sun Ray clients and Sun Ray Session Servers can also be encrypted using the ARCFOUR algorithm.

The Secure Network Access Platform allows site security policy to be easily mapped into the IT infrastructure. The security mechanisms in Trusted Solaris mesh well with traditional IT security precautions, including standard physical and personnel IT security measures. The Trusted Solaris Operating Environment can be easily configured to reflect underlying site security policy – for example, by defining system label ranges, security and administrative roles, and auditable events. The Secure Network Access Platform can be adapted to conform with specific security requirements and site policies.

High Availability

The Secure Network Access Platform Reference Architecture integrates components to produce an infrastructure designed for continuously available computing. In particular, hardware and software components from Sun Microsystems – Sun Fire V240 servers, the Trusted Solaris Operating Environment, Sun Ray Server Software, and the Secure Network Access Platform provisioning methodology – create an infrastructure that can help to minimize downtime and provide consistent levels of service.

For example:

- Sun Fire V240 servers contain built-in reliability features – hot swappable disk drives, redundant power supplies, and Advanced Lights Out Management

(ALOM). ALOM enables system managers to monitor server functions remotely.

- The Trusted Solaris Operating Environment offers proven reliability – it is deployed widely in classified environments to support mission-critical applications. It features a small, stable kernel design and load balancing across multiple processors, and incorporates administrative features that enhance manageability and reliability.
- Sun Ray Server Software configures servers in high-availability failover groups that permit load balancing and provide redundant thin client services. Figure 7 shows how redundant failover servers can connect to Sun Ray clients in the Secure Network Access Platform to enhance availability.
- Solaris JumpStart and the Secure Network Access Platform provisioning methodology can help to accelerate installation and recovery, especially for large numbers of servers. Server configurations can be replicated more easily and deterministically. If a server failure occurs, the software environment can be more quickly and reliably duplicated to a replacement.

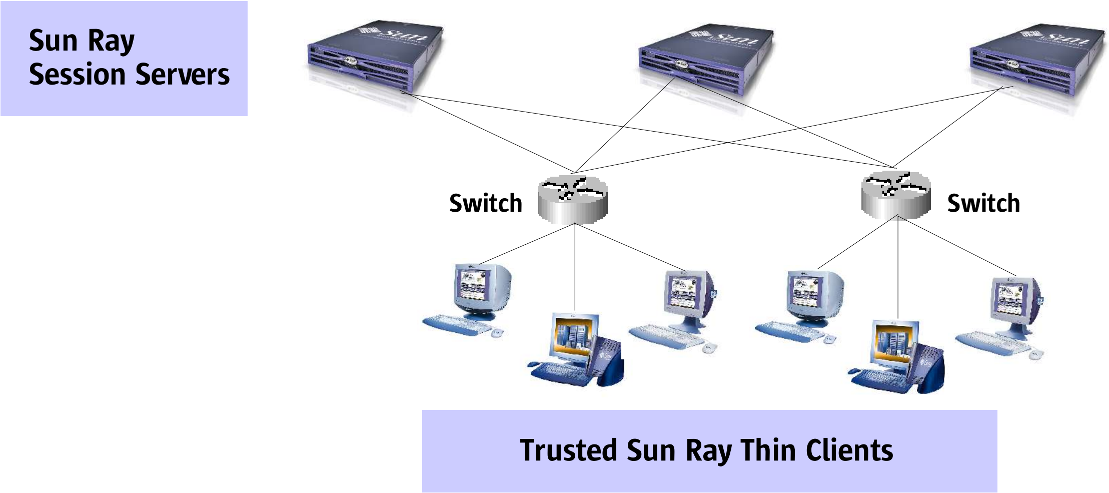


Figure 7. Failover groups/redundant Sun Ray servers.

Performance

Sizing a solution for growth over a period of time – according to the expected number and types of users – helps to ensure a reasonable level of responsiveness. The Secure Network Access Platform scales well, allowing additional users to be added incrementally and performance requirements to be met and maintained over time.

One architectural feature that contributes to responsiveness is built-in load balancing through the Sun Ray Server Software. When a user initiates a session on a Sun Ray thin client, the software directs the Sun Ray appliance to the server in the failover group with the lightest load. If a server failure occurs, the software on the remaining servers attempts to distribute the failed server's sessions evenly among the remaining systems. The load balancing algorithm takes into account each server's capacity (the number and speed of its CPUs) and its existing load, so that larger or less heavily loaded servers can host more sessions.

Scalability

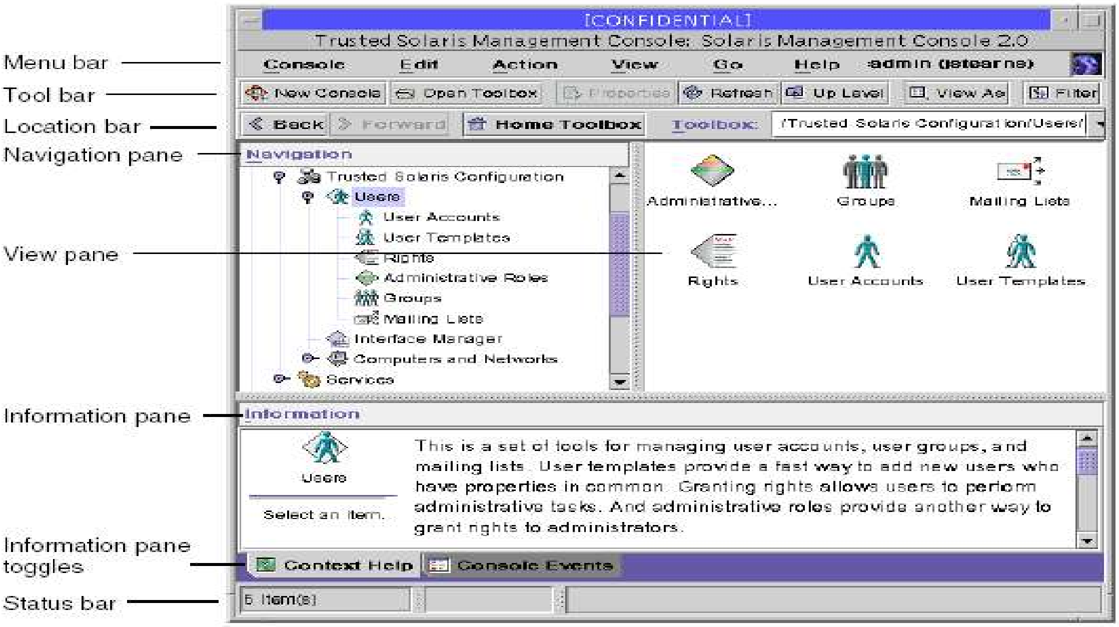
The Secure Network Access Platform is designed to scale to accommodate small, medium, and large deployments. It is primarily designed to scale horizontally rather than vertically.

Vertical scaling allows resources (such as CPUs, memory, and I/O cards) to be incrementally added to a server to increase processing capacity. For example, a second processor and up to three PCI network cards can be added to a Sun Fire V240 server. Other Sun servers – such as the Sun Fire V880 with up to 8 processors and 64GB of memory, or the Sun Fire V1280 server with up to 12 processors and 96GB of memory – offer a greater degree of vertical scalability. Because Sun's SPARC-based servers are binary compatible, these servers can be used as alternatives to Sun Fire V240 servers in deploying the Secure Network Access Platform Reference Architecture.

Horizontal scaling replicates services across multiple physical servers, allowing service delivery to occur from multiple systems. Horizontal scaling enhances responsiveness as user populations grow, and provides redundancy that can improve application availability. The Secure Network Access Platform Reference Architecture easily scales horizontally – additional Sun Fire V240 servers can be added as Sun Ray Session Servers (Figure 5).

Manageability

Administration in the Trusted Solaris Operating Environment relies on many of the same tools as in the standard Solaris Operating Environment, including the Solaris Management Console (SMC). SMC is a GUI-based “umbrella” application (Figure 8) that serves as a launching point for administrative tools.



This is a set of tools for managing user accounts, user groups, and mailing lists. User templates provide a fast way to add new users who have properties in common. Granting rights allows users to perform administrative tasks. And administrative roles provide another way to grant rights to administrators.

Figure 8. Trusted Solaris features an administrative interface based on the Solaris Management Console.

In the Trusted Solaris Operating Environment, several administrative roles exist by convention: the System Administrator role, which creates user accounts, and the Security Administrator role, which sets up security-related aspects of an account. Each role is authorized to access certain SMC-based administrative tools. For example, the System Administrator is authorized to run the SMC User Accounts tool, which provides two ways to create a user – from scratch using a "wizard", or from a template. These and other roles can be created to facilitate accountability for specific administrative tasks.

The Secure Network Access Platform offers enhanced manageability through the use of stateless Sun Ray thin clients. These “ultra-thin” appliances require no desktop administration, unlike stateful PCs that are prone to virus attacks. All thin client configuration tasks – such as defining failover groups and enabling encryption – are centralized at the Sun Ray Session Servers. The Sun Ray Server Software also features an easy-to-use, GUI-based administrative tool.

Monitoring the health of systems and networks can help administrators anticipate problems and proactively respond. The Sun Ray Server Software includes a module that interfaces to Sun™ Management Center software, a tool that Sun offers to monitor all Sun infrastructure elements. The Sun Management Center software creates a remote single point of management for all Sun components – including Sun Ray thin clients and failover groups, Sun Fire servers, Sun storage components, and the Solaris Operating Environment. In the Secure Network Access Platform, authorized system managers can use Sun Management Center, which can be installed on the Sun Blade 150 workstation, to track server performance, server hardware, and the state of system resources. Sun Management Center can also integrate with existing third-party enterprise management platforms (Computer Associates' Unicenter TNG, HP's OpenView VantagePoint Operations, or Tivoli's TES).

Infrastructure and Architectural Considerations

This section briefly describes infrastructure considerations that should be taken into account when planning an Secure Network Access Platform deployment. Sun Services consultants (or an experienced systems integration partner) can help customers define requirements for the IT infrastructure, specifying goals for security, high availability, performance, scalability, and manageability.

Networking

In a Secure Network Access Platform implementation, network design is critical to achieve both security and performance-related goals. In each Sun Ray Session Server, a dedicated network interface is required for each classified network (Figure 5). This design facilitates the necessary security containment. Some sites may require connections to a large number of networks, requiring each server to be configured with a large number of network interfaces. In some deployments, higher-end Sun servers may be needed to support the required number of network connections. Switched connections to the classified domains simplify network cabling and configuration.

To facilitate performance on the Sun Ray thin clients, a Gigabit Ethernet switch is recommended to connect the Sun Ray Session Servers in the failover group. Switched 100Base-T links are used to interface to the Sun Ray thin clients.

If desired, ARCFOUR encryption between the thin clients and Sun Ray Session Servers can be configured according to one of these options:

- for upstream traffic only
- for downstream traffic only
- for bidirectional traffic

In addition, server-side authentication can be enabled through pre-configured public-private key pairs in the Sun Ray Server Software and Sun Ray firmware. The Digital Signature Algorithm (DSA) can be used to verify that clients are communicating with a valid Sun Ray server. This authentication scheme can help to mitigate trivial man-in-the-middle attacks and make it harder for attackers to spoof the Sun Ray Server Software.

Sun Server Configuration

As shown in Figure 5, the Secure Network Access Platform features two primary server configurations:

- Sun Ray Session Servers
- Install Servers

Sun Ray Session Server sizing is generally based on a number of factors, including: the number supported users, the number of required network interfaces, the number of labels defined, application workloads, and auditing profiles. Since the Secure Network Access Platform Reference Architecture is flexible and scalable, it can easily be modified to provide reasonable responsiveness.

The architecture encourages a distributed approach to service delivery. Multiple Sun Ray Session Servers and the use of failover groups enable redundancy that can enhance service availability. In configuring Sun Ray Session Servers in the infrastructure, care should be taken to provide redundant DHCP and NIS+ services. In the event of a failed DHCP server, redundant DHCP services can still allow IP addresses to be assigned to Sun Ray thin clients. In the reference implementation, the Secure Network Access Platform Install Server is configured as the NIS+ master, and the Sun Blade 150 Management Station is configured as an NIS+ replica server.

The Secure Network Access Platform Reference Architecture assumes that applications use legacy storage resources. A minimal amount of local storage is required on each Sun Ray Session Server, primarily for the operating environment, thin client swap space, and run-time software. In addition, a second internal disk is configured on the Sun Fire V240 servers for audit trail storage.

The Secure Network Access Platform Install Server requires local storage for the Trusted Solaris Operating Environment, as well as storage for the packages required for JumpStart installations.

Thin Client Limitations

In the Secure Network Access Platform Reference Architecture, Java Card applications are not supported on Sun Ray thin clients. However, thin client users can use generic smart cards to facilitate hot desking. With smart cards, users can switch to any thin client in the LAN, allowing users to access the same applications from any desktop. Note that hot desking functionality is only available in conjunction with smart card use.

Provisioning Methodology

Implementing the Secure Network Access Platform offers customers the benefits of a tested and proven solution. IT managers can count on a low-risk solution – one that can reach business goals and be deployed quickly, with less chance of cost and schedule overruns. The provisioning methodology used to deploy the Secure Network Access Platform plays a major role in minimizing risk and reducing time-to-deployment.

The provisioning methodology relies on Trusted Solaris JumpStart technology, which can help administrators replicate server configurations more easily and consistently in Secure Network Access Platform implementations. A dedicated Secure Network Access Platform Install Server – a Sun Fire V240 server with the Trusted Solaris Operating Environment (Figure 5) – can be used to JumpStart-install large numbers of Sun Ray Session Servers. JumpStart can load the Trusted Solaris Operating Environment on those machines, install recommended patches, and execute "finish" scripts to fine-tune the initial installation. Scripts can be used to replicate security-relevant databases (label definitions, network configurations, rights profiles, etc.), or to minimize and harden the operating environment.

Sun Services

Consultants from Sun Microsystems, Inc. are skilled at designing and building scalable IT infrastructures for mission-critical networked applications. Sun Services consultants can assist system integrators or customers in implementing the Secure Network Access Platform Reference Architecture and tailoring the provisioning methodology to meet site requirements.

Most data centers have stringent goals for uptime, data availability, scalability, total cost of ownership, and investment protection. Components in the Secure Network Access Platform address many of these data center issues. Sun consultants are available to offer additional consulting, staff assessment, training, and design services to help customers meet specific data center goals. Sun Services consultants can assist customers with installation, optimization, and application integration tasks in deployments based on the Secure Network Access Platform Reference Architecture.

Summary

Sun understands the IT challenges faced by government agencies striving to enforce stringent security requirements while trying to facilitate more effective information sharing. With years of experience deploying networked computing architectures, Sun developed the Secure Network Access Platform to provide users in classified environments with a single access point to multiple security compartments and classifications. The Secure Network Access Platform architectural model eliminates the inefficiencies of a “stovepiped” application architecture that often uses multiple fat-client desktops to access data in each compartment.

The Secure Network Access Platform relies on a thin-client, trusted computing model that combines best-of-breed hardware and software components from Sun and third parties. Leveraging the existing infrastructure and legacy applications, it delivers a proven solution focused on compartmentalized security and low total cost of ownership. The architecture takes into account critical IT design criteria such as security, high availability, performance, scalability, and manageability.

Key to implementing the Secure Network Access Platform is the provisioning methodology used to deploy it in a proof-of-concept setting. This provisioning methodology can help Sun customers and system integrators implement the Secure Network Access Platform more quickly, more deterministically, and with less risk. Consultants from Sun Services have significant expertise in designing networked computing infrastructures, and can help customers tailor the Secure Network Access Platform to meet specific business and security goals.

References

Sun Microsystems posts product information in the form of data sheets, specifications, and white papers on its Internet Web site at http://www.sun.com. Look for these and other white papers:

- Trusted Solaris with Sun Ray Ultra Thin Client – The JICPAC Experience, 2003.
- Sun Fire V210 and Sun Fire V240 Server Architecture, March 2003.
- Sun Ray Overview, April 2003.
- Accessing Microsoft Windows Functionality from the Solaris Operating Environment, January 2000.
- Sun Ray Interoperability Brief, August 2003.
- Server Grouping for the Sun Ray 1 Enterprise Appliance White Paper, March 2000.
- Server Virtualization with Trusted Solaris 8 Operating Environment, February 2002.
- Maintaining Network Separation with Trusted Solaris 8 Software, 2001.

Sun product documentation is available from http://docs.sun.com. Look for the following product documentation related to the Secure Network Access Platform Reference Architecture:

- Trusted Solaris 8 HW 7/03 Answerbook, including the Trusted Solaris Administration Overview
- Sun Ray Server Software 2.0 Administrator's Guide

Other Web sites related to the Secure Network Access Platform Reference Architecture include:

- Citrix Systems, Inc., http://www.citrix.com
- Common Criteria, http://csrc.nist.gov/cc

Glossary

authorization

Permission granted to a Trusted Solaris user to perform an action that would be otherwise prohibited by security policy.

failover group

A group of servers configured by the Sun Ray Server Software that can provide thin client services whenever a Secure Network Access Platform Sun Ray Session Server goes offline. Thin client sessions are assigned to a server within a failover group to perform load balancing.

label

A string indicating the security level of an entity (file, directory, process, device, or network interface) in Trusted Solaris and used to determine whether access should be permitted. There are two components to a label: a classification indicating the hierarchical level of security, and zero or more compartments that define who has a need to the entity given a sufficiently high classification.

mandatory access control (MAC)

A Trusted Solaris-enforced access control mechanism that uses clearances and labels to enforce security policy.

rights profile

A means of bundling authorizations, commands, and privileged operations for certain users and roles in Trusted Solaris.

privilege

A permission granted to a program by the Trusted Solaris security administrator to override some aspect of security policy.

thin clients

Thin clients allow all computing to be done remotely. Sun Ray thin clients are completely stateless, meaning they have no locally resident data, applications, or operating system.